Review Paper on Vajra: A Block chain Based Payment Platform by NPCI

Shivam Soni, Risahbh Soni

Abstract— **Distributed Ledger Technology (DLT) has emerged as one of the most important and disruptive technologies in the last decade. It has the potential to change the way people do their business, transact their assets, and control their personal data. Though the concept of DLT was first implemented in 2009 as Bitcoin, it has gained significant attention over the past few years. During this time, different DLT enthusiasts and commercial companies have the advantage of developing several DLT platforms. These platforms are usually categorized as public vs private, general-purpose vs application-specific and so on. As a growing number of people are interested to build Distributed LedgerTechnology applications, it is important to understand their underlying architecture and mechanism in order to determine which DLT platform should have the best use-case for a specific DLT application. In addition, the platforms need to be checked and analyzed to assess their applicability, resiliency, and sustainability in the long run. In this paper, we have compared several leading DLT platforms and analyzed their capabilities based on several quantitative and qualitative criteria. The analysis presented in this paper will help the DLT developers and enthusiasts to choose the best platform as per their requirement(s).**

***Index Terms*— hashgraph, distributed ledger , consortium block chain, consensus protocol**

I. INTRODUCTION

DLT is a new technology with great potential. It promises to provide highly secure tamper-evident transactions that can be stored in a distributed database and is versatile enough to be adapted to various cases.

Following are the Key benefits of using DLT in the payment industry:

- Less reconciliation of transactions, higher resilience, and efficiencies through automation and transparency
- Real-time clearing and settlement processes
- Minimizing operations and have less financial risks
- Economical, tamper-proof, secure and accessible
- Provides a legitimate audit trail

VAJRA PLATFORM– A Distributed Ledger system introduced by **National Payment Corporation of India** for automated payment, clearing & settlement.

Manuscript received February 12, 2020

Shivam Soni, B.tech Department of Computer Engineering, Lakshmi Narayan Collage of Technology and Science, Affiliated to RGPV University, Bhopal

Risahbh Soni, B.tech. Department of Computer Engineering, Lovely Professional University, Jalandhar, Punjab

The main aim of discussing the topic of the vajra platform is to strengthen the potential use case of distributed ledger technology in the payment industry

Discussion about the implementation of different consensus algorithms used in distributed ledger systems to make it more automated and relevant to the payment industry.

II. LITERATURE SURVEY

Node is the most important and fundamental component of a DLT. The clearing-house node (NPCI), the participant nodes (Bank's/ASP/PPI/PSP) and Notary node(UIDAI node) will be treated as participants of the vajra platform.

PARTICIPANT NODE

Banks such as Application service provider/payment service provider/Payment protection insurance on the Vajra platform will be the participant nodes. These nodes can post, receive and view transactions on the platform.

For example, for a particular transaction involving 2 banks and 2 PSPs, only the concerned 4 Promissory nodes will post and receive transactions. All other banks such as the application service provider on Vajra will be able to only view the header info.

CLEARING HOUSE NODE

The clearinghouse node will have the Admin rights to this platform and will be maintained by the National payment corporation of India. It will provide a root-authority-signed TLS certificate from the network's permission service to the participant nodes.

NOTARY NODE

The notary node will validate a transaction only if Aadhar biometric is used for authentication. It will receive transactions only from the C-H Node

CONSENSUS ALGORITHM

A consensus algorithm is a procedure or a way through which all the nodes in the Blockchain network reach a **common agreement** about the present or actual state of the distributed ledger. In this way, consensus algorithms achieve reliability in the network and establish trust between unknown nodes in a distributed computing environment.

By reaching the consensus the block which acts as a ledger has been added to the blockchain.

example of various type of consensus algorithm as follows:-

- ✓ proof of work
- ✓ proof of stake
- ✓ delegated byzantine fault tolerance
- ✓ delegated proof of stake

One of the biggest challenges that most distributed systems face is reaching to a consensus. This problem is usually called "Byzantine General's Problem".

So What is the Byzantine General's Problem?
Byzantine General's Problem is a condition of a computer system, particularly distributed computer systems, where components may fail .Byzantine General's Problem leads to the major factor of not able to reach consensus in blockchain the reason is that no two nodes in the network are trustworthy to each other.
To resolves, this Byzantine General's Problem Satoshi Nakamoto, the creator of Bitcoin, was able to bypass the Byzantine General's problem by inventing the proof of work protocol. This is the proof-of-work protocol that is used by Bitcoin and as well as Ethereum. The problem with that is proof-of-work is extremely wasteful and inefficient energy-wise.

There are more consensus mechanisms out there that claim to solves the Byzantine General's Problem and are more efficient than a proof of work consensus algorithm. the new consensus algorithm came into a play called delegated byzantine fault tolerance which is been used as a consensus algorithm in NEO- An open-source blockchain decentralized application platform founded in 2014 by Da HongFei and Erik Zhang.

Now, What is DBFT?

Delegated Byzantine Fault Tolerance[3]: Consensus algorithm based on assigning roles to nodes to helps reaching consensus.
DBFT does not have miners instead, it has the node that is split into ordinary nodes and consensus nodes. the majority of the node in the network are just ordinary citizen nodes that can transfer or exchange asset but they don't participate in validating blocks consensus node has the power to verify each block written to a blockchain similar to how elected government officials would represent the majority of its constituent.

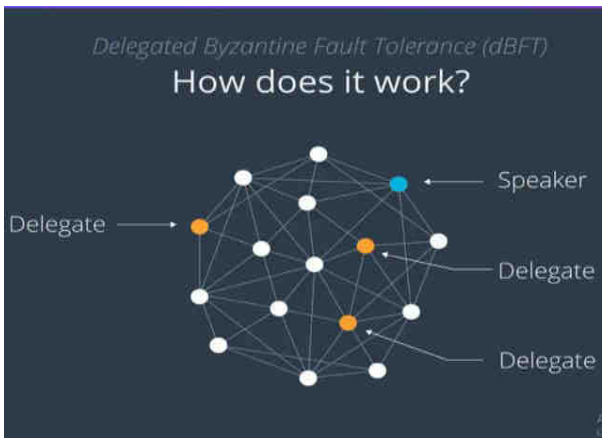


Fig1.1
for an ordinary node to become a consensus node it usually needs to meet certain criteria that differ from platform to platform

when its time to decide which block should be added next, a consensus node is randomly selected from the pool of all consensus node.

In the NEO blockchain, this chosen node is called a speaker and all the other consensus node are called delegates the speaker create new block and proposed it to the delegates two-thirds of all the delegates need to prove this block before it's passed if it doesn't pass, the chosen speaker return to being a normal delegates and another speaker is chosen

DBFT is said to be much faster than a proof of work and it requires fewer resources because there is no complicated cryptographic puzzle to solve.

In this paper, the author has precisely compared the different consensus algorithms and found that the DBFT consensus algorithm is best suited for the vajra platform here are the points that explain why?

- The clearinghouse node will have the Admin rights to this platform and will be maintained by NPCI this acts as a speaker node(in DB FT protocol) who has a right too elect
- In the vajra platform, only the parties who have been approved by the Network Administrator can be a part of the network which acts as delegates as per DBFT consensus protocol
- participant node in the vajra platform which are banks such as ASP(application service provider) /PSP(payment service provider) /PPI(payment protection insurance) acts as a delegates node as per DBFT consensus protocol which has access to post, receive and view.
- the clearinghouse node should have two-thirds of a majority vote to acts as a speaker node and have the admin rights and this speaker is chosen by the delegates.

Implementation of delegated Byzantine fault tolerance consensus protocol in the vajra platform resulted in more secured automated payments and acts as a purely distributed system by following certain specified rules of delegated Byzantine fault tolerance consensus protocol.

SMART CONTRACTS

A Smart Contract is a self-executable and self-enforcing agreement or contract that not only executes the plan but also manages the plan and its transaction costs embedded in computer code managed by a blockchain. The code contains a set of rules under which the parties of that smart contract agree to interact with each other. Smart contracts provide mechanisms for efficiently managing assets and access rights between two or more parties.

In the vajra platform, the Smart Contracts which is running on the DLT platform validates transactions against defined business rules and triggers transactions based on rules.
smart-contract plays an important role in the real-time payment settling process and reduces manual processing FTE for reconciliation.

CONSORTIUM BLOCKCHAIN

Consortium Blockchain is also known as a permission blockchain. It is the features of both private and public blockchain. It is a distributed system, unlike decentralized, public blockchain. In Consortium blockchain, control is given only to a few predetermined nodes. Here, any particular transaction is limits to its certain nodes.

Consortium blockchain is partially decentralized and These blockchains are faster and more scalable. vajra platform is based on a consortium blockchain Because the existing system is mostly centralized it became quite hard to directly move the step forward towards the decentralized/distributed system for that consortium blockchain have the best use case

III. KEY FEATURE OF DLT

A. Distributed Ledger

It is a database apprehended and modernized by every contestant in a bulky association. It represents how information is stored and gathered. Every single node on network process every transaction and concludes it with some final conclusion. Then, voting is done on those conclusions to make a mainstream agree with the conclusion. The disseminated Ledger has been modernized, and all nodes preserve their own indistinguishable copy of the ledger.

B. Digital Signature

A digital signature is a mathematical technique used to validate or verify the authenticity and honesty of a message, software or digital data.
It's simply the verification that the message sent by the sender is been sent by the sender or not.

C. Cryptographic hash function

A cryptographic hash function is hash function which takes an input or a message and returns a fixed-size string of bytes. The string is also known as digital fingerprint, message digest.

D. Consensus Protocol

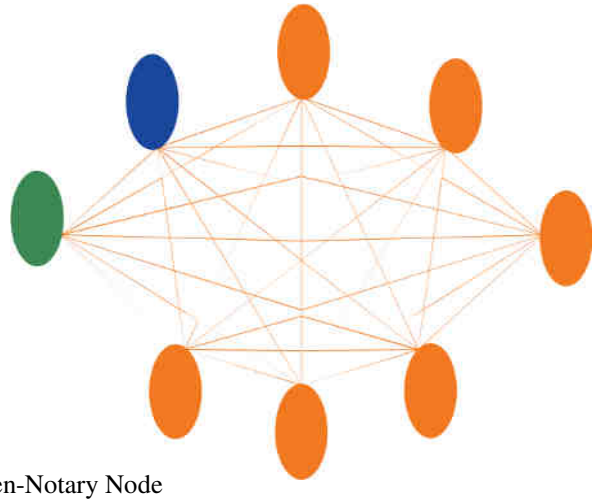
Consensus protocol are a decision-making process for a group, where individuals of the group make and support the decision that works best for the group. It's a form of resolution where individuals need to support the majority decision, whether they liked it or not.

IV. ARCHITECTURE OF VAJRA

The Vajra platform will be accessed by multiple entities for performing transactions. The bank nodes will get requests from APIs and will process it on Vajra. The system will have self-executing contracts called a smart contract containing specified business rules. After successful completion of the requests, the on-chain data (eg. Hashes of the transactions) will be added to the distributed ledger.

The Clearing House Node has the power to add new nodes on the platform. Every outsourced party that interacts with the participants of the platform will be authenticated by the node. Vajra takes care of API intercommunication with key management and defined security procedures and security in data access

O Chain database will be used to store information that is not published on the platform
only the node in the network has the permission to access the data in the network
Each participant node in the vajra network maintains a ledger of their own.



Green-Notary Node
Blue-Clearing House Node
Orange-Participant Node

Fig 1.2

There are three types of nodes on the platform:

- Clearing House node (CHN) for NPCI
- UIDAI node for Aadhaar authentication
- Participant node (PN) for all banks/ASP/PPI/PSP

*UIDAI node will only be used in case of biometric authentication.

KEY BENEFITS OF VAJRA IN PAYMENT , CLEARING AND SETTLEMENT

- Transparency:

Real-time visibility into the state of a transaction can help reduce problems and improve operations at banks and NPCI.

- Information Storage

Disparate file systems maintained across banks, NPCI and other participants lead to a lot of reconciliation challenges and problems. Hence, decentralized and distributed data storage would help reduce the pain of reconciliation across all the participants.

- Time Sensitivity

Real time transaction will reduce the clearing and settlement process cycle.

KEY ADVANTAGES OF USING DLT

• **Cost Reductions**. Digital ledger technology has the efficiency for significant cost reductions due to removing the need for reconciliation as DLT systems by definition contain the shared truth and hence there is no need to reconcile one version of "truth" with that of one's counterparties

• **Greater transparency and easier auditability**. All network members have a full copy of the distributed ledger.

Changes can only be made when consensus is established and they are sent across the entire network in real-time.

• **Immutability and verifiability**. DLT can provide a tamper-proof and verifiable audit trail of transactions of any digital or physical asset.

• **Gains in speed and efficiency**. DLT has the potential of increasing speed and lowering inefficiencies by reducing friction in transactions or real-time clearing and settlement processes by removing intermediaries and automating processes.

V FUTURE DISCUSSION

HASHGRAPH

Hashgraph is a distributed ledger technology developed by Leemon Baird, the co-founder of Swirlds. It is an asynchronous Byzantine Fault Tolerence (aBFT) consensus algorithm that they consider capable of securing the platform against attacksIt does not use miners to validate transactions, and uses directed acyclic graphs for time-sequencing transactions without bundling them into blocks.

THE SWIRLDS HASHGRAPH CONSENSUS ALGORITHM

• **Gossip about gossip** - the hashgraph is spread through the gossip protocol. The information being gossiped is the history of the gossip itself, so it is “gossip about gossip”. This uses very little bandwidth overhead beyond simply gossiping the transactions alone.

CONCLUSION

We have conducted comprehensive survey on Distributed Ledger Technology. Distributed Ledger Technology is an budding solution for decentralized finance(de-fi) without the need of a trusted third party.

Data on blockchain gets stored in a block over the public ledger, which means that every participant has a copy of the entire Few Advantages and Disadvantages have been seen and various applications of Blockchain Technology are stated. Most Importantly, Future of the Blockchain has been predicted if few of the assumptions comes true, then what are the possible technologies which can be created by blockchain technology. Concepts like consensus, distributed ledger, delegate byzantine fault tolerance, hashgraph DLT, etc. have been explained in short. Other than the Blockchain concepts, working and future predictions Bitcoin has been viewed as the best example for Blockchain as it the first cryptocurrency to bring the blockchain technology to real.

REFERENCES

[1] M. J. M. Chowdhury et al., "A Comparative Analysis of Distributed Ledger Technology Platforms," in IEEE Access, vol. 7, pp. 167930-167943, 2019.

[2] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

[3] T. Crain, V. Gramoli, M. Larrea and M. Raynal, "DBFT: Efficient Leaderless Byzantine Consensus and its Application to Blockchains," 2018 IEEE 17th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, 2018, pp. 1-8.

[4] Z. Akhtar, "From Blockchain to Hashgraph: Distributed Ledger Technologies in the Wild," 2019 International Conference on Electrical, Electronics and Computer Engineering (UPCON), ALIGARH, India, 2019, pp. 1-6.

[5] https://hbarprice.com/hashgraph-technology-use-case-for-financial-services